

Please amend the following paragraphs of the specification in the manner indicated:

[0067] is readily demonstrated. For example, starting with the encryption element *Enc*

$$\left[ \left[ \prod_{1 \leq i \leq n} t(R_{TAi}, rQ_{IDi})^{b_i} = \prod_{1 \leq i \leq n} t(siP, rQ_{IDi})^{b_i} \right] \right]$$

$$\prod_{1 \leq i \leq n} t(R_{TAi}, rQ_{IDi})^{b_i} = \prod_{1 \leq i \leq n} t(siP, rQ_{IDi})^{b_i}$$


---

$$= \prod_{1 \leq i \leq n} t(rP, siQ_{IDi})^{b_i}$$

$$= t \left( rP, \sum_{1 \leq i \leq n} b_i siQ_{IDi} \right)$$

$$= t \left( U, \sum_{1 \leq i \leq n} b_i siQ_{IDi} \right)$$

$$= t \left( U, \sum_{1 \leq i \leq n} b_i si \right)$$

Please replace Figure 3 with the amended version of same enclosed herewith. The identity and TA elements of the decryption key (private - in the dashed line box) for the first embodiment used the term  $S_{IDi}$  whereas the description used the term  $S_i$ . See paragraph 0060. So in the amended figure, the term  $S_{IDi}$  is replaced with the term  $S_i$  in the first embodiment. Additionally,  $P_{publi}$  (second embodiment, general form) has been changed to  $P_{publi}$  to be consistent with the description (see paragraph 0072).